

From: Julio Nuldemar <julionuldemar@hotmail.com>
Sent: Tuesday, 16 June 2026 22:27:26
To: atencioncliente <atencioncliente@crcom.gov.co>
Subject: COMENTARIOS PROYECTO RESOLUTIVO

Bogotá D.C., 16-06 de 2026

Señores: COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC) E. S. D.

ASUNTO: Proyecto de Resolución *“Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles”*.

Respetados Comisionados:

CAPÍTULO I: CARGOS DEFINITIVOS DE OPOSICIÓN TÉCNICO-JURÍDICA

CARGO PRIMERO: Vicio de Falsa Motivación por Incongruencia Lógica Absoluta en el Mecanismo de la Cuarta Etapa

El texto propuesto para la *“Cuarta etapa — Restricción temporal del servicio de mensajería”* dispone que la restricción de envío de SMS:

“...se levantará automáticamente si no se han presentado nuevos eventos de detección. La restricción no afectará la capacidad del usuario de recibir mensajes de texto...”

- **Fundamentación Jurídico-Técnica:** La redacción de este aparte incurre en una contradicción lógica sustancial que se traduce en un vicio de **falsa motivación por imposibilidad física y técnica**. Si el operador (PRST) ejecuta el bloqueo de la capacidad de *envío* de SMS de una línea, el canal de originación queda totalmente cerrado en los nodos de la red. Al estar el canal cerrado, la probabilidad técnica de que la línea genere "nuevos eventos de detección de envío" es de cero (0).
- **Efecto Antijurídico:** Al ser imposible registrar nuevos eventos durante el bloqueo, la restricción técnica se levantará de forma automática e inexorable al séptimo día. Esto genera un incentivo perverso para las redes de fraude automatizado (*SIM-farms*), las cuales solo requerirán esperar el cumplimiento del plazo para reactivar el ataque. El texto, tal como está redactado, despoja a la medida de toda idoneidad y eficacia para combatir el fraude, configurando una carga operativa inútil para el operador.

CARGO SEGUNDO: Vulneración del Debido Proceso y Desviación de la Finalidad del Habeas Data en la Segunda Etapa de Notificación

La *“Segunda etapa — Notificación al usuario”* constriñe al operador a notificar la detección de un patrón atípico a través del canal de atención que el usuario haya habilitado (entendiéndose por este, según los antecedentes del proyecto, el canal seleccionado en la última PQR interpuesta por el usuario).

- **Fundamentación Jurídico-Técnica:** Esta disposición vulnera el **Principio de Finalidad** consagrado en el artículo 4 de la **Ley 1581 de 2012 (Habeas Data)**. Los datos de contacto capturados por un operador en el marco de la interposición de una PQR tienen una finalidad única, expresa y limitada: la notificación de la decisión que resuelve dicha reclamación (Resolución CRC 5050 de 2016). Utilizar dicha información para finalidades de control de tráfico, sospecha de fraude o medidas preventivas, sin el consentimiento previo, expreso e informado del usuario, constituye un tratamiento ilegal de datos personales.

- **Vulneración al Artículo 29 C.P.:** Asimismo, el proyecto ignora la realidad estadística del mercado: la gran mayoría de la base de usuarios de un operador jamás ha interpuesto una PQR. Al amarrar de forma exclusiva la notificación a este canal, la norma sitúa al operador en una imposibilidad material de notificación frente a la mayoría de sus clientes, forzando la aplicación directa de la restricción del servicio (Cuarta Etapa) sin que el usuario haya sido efectivamente advertido, rompiendo las garantías mínimas del debido proceso.

CARGO TERCERO: Ruptura de la Proporcionalidad Reguladora y Configuración de Objeto Imposible frente a los Operadores Móviles Virtuales (OMV)

El proyecto impone obligaciones simétricas y uniformes de monitoreo, detección de señalización anómala y ejecución de bloqueos instantáneos en la infraestructura core de red a todos los operadores por igual.

- **Fundamentación Jurídico-Técnica:** De acuerdo con la Ley 1341 de 2009 y la jurisprudencia constitucional, la regulación sectorial debe respetar el principio de proporcionalidad y razonabilidad. Los OMV se caracterizan por una condición técnica de subordinación operativa específica: carecen de elementos de red centrales (*Core Network*) y dependen contractualmente de la infraestructura del Operador Móvil de Red (PRM) anfitrión.
- **Objeto Imposible:** Un OMV no posee el control físico ni lógico sobre las capas de señalización profunda necesarias para interceptar, filtrar o detener de forma autónoma el tráfico. Imponerle obligaciones directas de bloqueo sobre infraestructura ajena configura un acto administrativo con **objeto imposible**, violando el principio general del derecho según el cual *a nadie se le puede obligar a lo imposible*, lo que vicia la legalidad de la resolución.

CARGO CUARTO: Ruptura del Principio de Neutralidad Tecnológica y Extralimitación de Funciones en la Regulación de Canales Propios y de Software

El proyecto prescribe un régimen de control absoluto sobre la mensajería a través del concepto de *"Plantilla de contenido A2P (Template ID)"*, determinando que:

"Ningún mensaje A2P podrá ser cursado a través de las redes de los PRST si no está respaldado por una plantilla de contenido aprobada y vigente en el sistema del validador centralizado."

- **Fundamentación Jurídico-Técnica:** Esta restricción absoluta viola el **Principio de Neutralidad Tecnológica** establecido en el artículo 2 de la Ley 1341 de 2009. Los operadores, en ejercicio de su libertad de empresa, han desarrollado canales digitales propios, cerrados y seguros para comunicarse con sus usuarios (v.gr., notificaciones *Push* en sus aplicaciones oficiales, canales Web o sistemas basados en Applets/STK en la tarjeta SIM). Al ser canales cerrados, controlados de punta a punta por el operador, el riesgo de suplantación de identidad o *spoofing* es inexistente.
- **Extralimitación de Competencias:** Someter la transmisión de datos informáticos internos de las aplicaciones de los operadores al control previo de un Validador Centralizado constituye una intervención desproporcionada en el desarrollo de software. Adicionalmente, al pretender que el validador audite las "condiciones de consentimiento requeridas", la CRC se extralimita en sus funciones e invade la competencia exclusiva de la Superintendencia de Industria y Comercio (SIC), única autoridad nacional de control para la protección de datos personales.

CARGO QUINTO: Indebida Exposición al Riesgo de Responsabilidad Civil por "Falsos Positivos" e Inexistencia de Cláusula de Inmunidad

Al exigir el bloqueo y filtrado perentorio de tráfico legítimo ante la simple coincidencia con "patrones atípicos" o desalineaciones de plantillas, la CRC altera el régimen de responsabilidad de los operadores.

- **Fundamentación Jurídico-Técnica:** El tráfico de mensajería A2P corporativo transita información de alta prioridad (alertas de fraude bancario, contraseñas de un solo uso [OTP] para transacciones de comercio electrónico, alertas de servicios de emergencia y notificaciones médicas). Si el algoritmo de

control o el Validador Centralizado incurren en un error de apreciación (falso positivo) y bloquean tráfico legítimo, se generarán cuantiosos perjuicios económicos a terceros.

- **Desequilibrio Regulatorio:** El proyecto de resolución omite establecer una cláusula de salvaguarda o inmunidad regulatoria que proteja el patrimonio del operador cuando este actúe de buena fe en cumplimiento de un deber legal de bloqueo. Al no preverlo, la CRC expone a los operadores a demandas multimillonarias por **lucro cesante y pérdida de la oportunidad** derivadas de los fallos del sistema automatizado, rompiendo el principio de confianza legítima.

CAPÍTULO II: PETICIONES CONCRETAS Y PROPUESTA DE ARTICULADO (TEXTO DEFINITIVO)

Con el fin de subsanar los yerros normativos demostrados y garantizar un marco ejecutable, solicitamos de manera expresa a la Comisión incorporar en el texto definitivo de la resolución las siguientes modificaciones sustanciales:

1. Modificación al Ámbito de Aplicación (Exclusión de Canales Propios y Comunicaciones Operativas)

Solicitamos que se excluya expresamente del ámbito de aplicación de la norma, del registro de *Sender ID* y de la obligación de plantillas, a las comunicaciones que el propio operador realice con su base de usuarios con fines informativos, de red o regulatorios, ya sea utilizando numeración convencional (MSISDN) o a través de sus canales y aplicaciones digitales propias.

- **Texto Alternativo Propuesto (Parágrafo del Artículo de Alcance):**

PARÁGRAFO NUEVO: Exclúyase del ámbito de aplicación de la presente resolución, y por ende de las obligaciones de registro de SENDER ID y validación previa de plantillas ante el Validador Centralizado, a las comunicaciones de naturaleza informativa, operativa, regulatoria o de atención al cliente emitidas directamente por los PRST (incluyendo Operadores Móviles Virtuales - OMV) hacia sus propios usuarios finales, bien sea que se utilicen recursos de numeración móvil convencional (MSISDN) o canales digitales propietarios independientes del canal SMS tradicional (notificaciones Push, Applets SIM u homólogos).

2. Modificación a la Cuarta Etapa (Subsanación de la Incongruencia de Red)

Solicitamos corregir la contradicción técnica del artículo relativo al levantamiento de la restricción, especificando que la ausencia de nuevos eventos se evaluará una vez se reestablezca la capacidad de envío, y no durante la vigencia del bloqueo técnico.

- **Texto Alternativo Propuesto:**

CUARTA ETAPA (Redacción Corregida): (...) La restricción tendrá una duración máxima de siete (7) días calendario, al vencimiento de los cuales se levantará temporalmente el bloqueo de envío. La medida se entenderá definitivamente superada si, dentro de los siete (7) días posteriores al levantamiento técnico de la restricción, no se registran nuevos patrones de tráfico atípicos asociados a la línea identificada.

3. Inclusión de un Régimen de Diferenciación por Rol en la Cadena de Valor (Protección al OMV)

Solicitamos radicar las obligaciones técnicas de monitoreo profundo, filtrado en capas de señalización y bloqueo de hardware exclusivamente en los agentes que ostentan el control físico y lógico del Core de Red.

- **Texto Alternativo Propuesto (Artículo Nuevo):**

ARTÍCULO NUEVO. ENFOQUE DIFERENCIADO POR ROL DE RED. Las obligaciones técnicas referidas al monitoreo de sistemas de señalización, control de originación de comunicaciones en capas profundas y ejecución material de bloqueos de tráfico forzoso

establecidos en esta resolución, serán exigibles única y exclusivamente a los PRST que ostenten el control físico, lógico y la titularidad de la infraestructura central de red (Core Network y elementos de acceso). Los Operadores Móviles Virtuales (OMV) quedarán eximidos de responsabilidad administrativa frente a fallas técnicas de filtrado que dependan de la infraestructura del operador anfitrión.

4. Inclusión de una Cláusula de Contingencia Técnica (*Fail-Safe*) para la Continuidad del Servicio

Solicitamos que la resolución prevea un mecanismo que impida la parálisis de las comunicaciones del país ante caídas del Validador Centralizado.

- **Texto Alternativo Propuesto (Parágrafo del Artículo del Validador):**

PARÁGRAFO NUEVO. PROTOCOLO DE FALLA SEGURA (FAIL-SAFE). En caso de presentarse indisponibilidad técnica, caídas de sistema, degradación de plataforma o fuerza mayor en el Validador Centralizado que impidan la verificación de plantillas en tiempo real, los PRST quedarán plenamente facultados para cursar de forma directa el tráfico A2P legítimo de sus clientes corporativos, priorizando el principio de continuidad del servicio público de telecomunicaciones. Durante el tiempo que dure la contingencia, se suspenderá la aplicación de sanciones por tráfico no validado.

5. Definición de Plazos Razonables y Régimen de Transición Gradual

Solicitamos sustituir los plazos de adecuación inmediata por un término técnicamente viable para la realización de desarrollos de software y pruebas de estrés en los sistemas de facturación y provisión.

- **Texto Alternativo Propuesto (Artículo de Transitoriedad):**

RÉGIMEN DE TRANSICIÓN: Las obligaciones derivadas del uso del Validador Centralizado y la verificación de plantillas entrarán en vigencia plena transcurrido un plazo no inferior a doce (12) meses, contados a partir de la fecha en que la CRC publique de manera oficial los manuales técnicos definitivos y las APIs de integración del Validador Centralizado. Durante los primeros seis (6) meses de dicho plazo, se adelantará una fase piloto obligatoria y no sancionatoria entre todos los agentes del mercado para la calibración del sistema.

Gracias.

JulioN